

# The Importance of PCI/CISP Certification

## Why Compliance Is No Longer Enough

The internet is an ever-evolving medium, much like a conversation that can be modified by anyone in the world. Most participants hope to inform and enrich the lives of others, but some participants enter the arena with malicious intentions. This latter group is growing in number and strength, armed with more tools than ever before. Your online business must now focus on protecting itself and the sensitive information of your customers. This is where PCI/CISP certification comes into play.

### What Is PCI/CISP?

The Payment Card Industry (PCI) is a joint creation of Visa, MasterCard, Discover and American Express. In response to the growing frequency and severity of credit card and identity theft, this organization created the PCI Data Security Standard (PCI DSS), with the overall goal of protecting credit card data wherever it may reside.

The Cardholder Information Security Program (CISP) was initiated and mandated by Visa in June 2001 by Visa. In 2004, these requirements were incorporated into the PCI DSS to establish industry wide standards for card security. These standards must be followed by both merchants and providers.

Sources: Visa Cardholder Information Security Program

### Why Is This Important?

Identity theft is a major issue that is growing exponentially. The FTC estimates that approximately nine million Americans have their identity stolen each year, a crime amounting to \$45 billion.

## Overview

#### 1. What is PCI/CISP?

PCI stands for the Payment Card Industry and CISP is the Cardholder Information Security Program, initiated by Visa.

#### 2. Why is this important?

Identity theft is on the rise, especially online. PCI/CISP certification provides the highest level of security possible to protect your business.

#### 3. Compliance vs. Certification?

Compliance means a provider only follows the guidelines of PCI DSS. Certification indicates verification from Visa itself, along with independent on-site audits.

#### 4. What do I need to do to remain certified?

Pick a PCI/CISP certified provider and perform self-scans and audits.

#### 5. Hosted, Open Source, or Licensed Solution?

Each has their differences. Hosted solutions are the most efficient way to become PCI/CISP certified.

#### 6. Why Volusion?

Volusion is fully PCI/CISP certified, provides additional security measures and monitors your site 24x7.

PCI compliance is critical for anyone doing business online, including the merchant and the customer. For the merchant, the penalties of using a non-PCI compliant provider can include:

- \$500,000 in fines (per incident)
- Complete loss of ability to process card transactions
- Class-actions lawsuits
- \$10,000 in monthly fines
- Major public relations crises

For the customer, credit card and/or identity theft is devastating. Dozens of calls must be made, dozens of forms must be filled and credit can be ruined. More important to your business, your customer has a new sense of mistrust that makes them weary to purchase with you online.

Sources: Federal Trade Commission, Washington Post, Javelin Strategy and Research

## What Is the Difference Between Compliance and Certification?

*PCI/CISP compliance* indicates that a merchant simply follows the PCI DSS guidelines. This means there is a wide spectrum of security measures that would qualify a business as compliant. Also, compliance is only measured once a year, so rapid-spreading malware and hacking innovations are not always addressed. In sum, there is a lack of accountability with compliance and it is no longer stringent enough to protect your most valuable asset – your business.

*PCI/CISP certification*, on the other hand, is a higher degree of guaranteed security. In order to be certified, a provider must make major investments in their servers and hardware to meet higher security standards. When this has taken place, there is a rigorous screening process to be listed on Visa's certification list. Additionally, PCI/CISP certified

“ PCI Certification is essential for any online business at this point in the game. We decided to invest millions to beef up our security infrastructure because we had to. The risk far outweighed the investment for us and our clients. ”

Clay Olivier, Volusion COO

companies are required to have an independent auditor come to their physical location to thoroughly inspect the security implementation.

## The vast majority of shopping cart solutions has not reached the level of PCI/CISP certification.

Merchants using these non-certified solutions face the greatest amount of risk because it is easier for hackers to access sensitive customer information. Most of these providers are unable to achieve certification because of the following:

- They do not have the necessary capital to complete certification requirements
- They are not knowledgeable enough to configure and code certification requirements
- They do not meet Visa's minimum company size requirements

Volusion is a fully PCI/CISP certified company. Check the status of your provider on Visa's list at: <http://usa.visa.com/download/merchants/cisp-list-of-pcidss-compliant-service-providers.pdf>. If they are not listed, your business is not adequately secured.

Source: Visa Cardholder Information Security Program

## What Do I Need to Do to Remain Certified?

PCI/CISP certified solutions have completed the overwhelming majority of the work; however there are still measures that must be taken from the business level. In order to be fully certified at the merchant level, your team must do the following:

- Select a PCI/CISP certified solution.
- Complete the Self Assessment Questionnaire (SAQ) once a year. The SAQ is a list of questions about your website and current security practices.
- Complete a vulnerability scan through an approved scanning vendor (ASV) periodically throughout the year. Then, provide documentation that your site passed the scan.

You can find the SAQ and list of ASVs online at: <https://www.pcisecuritystandards.org/>.

Sources: PCI Security Standards Council

## Hosted, Open Source, or Licensed Solution?

### Hosted Solutions

Using an ecommerce provider that is fully hosted and PCI/CISP certified provides the most efficient and cost effective method of achieving certification for your own website. This is because the provider has already completed the effort required to achieve this status, so your business automatically falls into this level of security certification.

Most hosted solutions are not PCI/CISP compliant or certified, so ensure your business inquires about the security level when searching for ecommerce providers.

### Open Source Solutions

Open source ecommerce solutions require hosting on your servers or procure hosting with another provider. This means that all measures to reach PCI/CISP certification fall under the responsibility of the business owner, which is a large capital and human resources investment.

### Licensed Solutions

Licensed ecommerce solutions also require your business to find a hosting provider, either in-house or from a third party. With this type of solution, your IT team must handle all certification efforts or pay a premium to be hosted with an entity that has reached this security level.

## Why Volusion?

Volusion is a fully hosted, fully PCI/CISP certified ecommerce provider, offering the highest level of security possible. The company also offers a 99.99% uptime guarantee with 100% redundancy of all network hardware, systems and data. In addition to being PCI/CISP certified, all sites are protected by dedicated, dual firewalls and equipped with leading proactive anti-virus tools. Your website is also placed on multiple servers, all housed in secure, unmarked facilities with 24x7 surveillance. Volusion is focused on safeguarding your online business so you can focus on growing it.

Our dedicated account managers and round-the-clock ecommerce experts are ready to learn more about your business and discuss your security concerns. Give us a call at 1.800.646.3517, opt. 7 or send an e-mail to [enterprise@volusion.com](mailto:enterprise@volusion.com) to schedule a consultation today.